CALIFORNIA ATTORNEY GENERAL'S LEGAL ADVISORY ON THE APPLICATION OF EXISTING CALIFORNIA LAWS TO ARTIFICIAL INTELLIGENCE

The California Attorney General's Office (AGO) issues this advisory to provide guidance to consumers and entities that develop, sell, and use artificial intelligence (AI)[1] about their rights and obligations under California law, including under the state's consumer protection, civil rights, competition, and data privacy laws.[2]

ARTIFICIAL INTELLIGENCE HOLDS GREAT POTENTIAL AND GREAT RISKS

AI systems are at the forefront of the technology industry, and hold great potential to achieve scientific breakthroughs, boost economic growth, and benefit consumers. As home to the world's leading technology companies and many of the most compelling recent developments in AI, California has a vested interest in the development and growth of AI tools. The AGO encourages the responsible use of AI in ways that are safe, ethical, and consistent with human dignity to help solve urgent challenges, increase efficiencies, and unlock access to information—consistent with state and federal law.

While AI tools present new opportunities, the use of AI can run the risk of exacerbating bias, discrimination, and the spread of disinformation, creating opportunities for fraud and causing harm to California's people, institutions, infrastructure, economy, and environment. For AI systems to achieve their positive potential without doing harm, they must be developed and used ethically and legally. Existing California law provides a host of protections that may be applicable to the development and use of AI tools.

Consumers must have visibility into when and how AI systems are used to impact their lives and whether and how their information is being used to develop and train systems. Developers and entities that use AI, including businesses, nonprofits, and government, must ensure that AI systems are tested and validated, and that they are audited as appropriate to ensure that their use is safe, ethical, and lawful, and reduces, rather than replicates or exaggerates, human error and biases. Developers and users must understand any risks involved in the use of AI, and ensure that AI is not used in a manner that causes harm to individuals, entities, infrastructure, competition, or the environment, or to the public at large.

AI systems are proliferating at an exponential rate and already affect nearly all aspects of everyday life. Businesses are using AI systems to evaluate consumers' credit risk and guide loan decisions, screen tenants for rentals, and target consumers with ads and offers. AI systems are also used in the workplace to guide employment decisions, in educational settings to provide new learning systems, and in healthcare settings to inform medical diagnoses. But many consumers are not aware of when and how AI systems are used in their lives or by institutions that they rely on. Moreover, AI systems are novel and complex, and their inner workings are often not understood by developers and entities that use AI, let alone consumers. The rapid deployment of such tools has resulted in situations where AI tools have generated false information or biased and discriminatory results, often while being represented as neutral and free from human bias.

Entities that develop or use AI systems must ensure that they and their systems comply with California law, including laws protecting consumers from unfair and fraudulent business practices, anticompetitive harm, discrimination

1 While the definition of AI may vary depending upon the context, for the purposes of this advisory, AI includes "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—(A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action." (15 U.S.C. § 9401(3).) California has also recently passed a law defining the term in certain instances as "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments." (See Gov. Code § 11546.45.5 et seq., added by AB 2885, Stats. 2024, ch. 843.)

2 This advisory provides the AGO's guidance on general application of California law to AI. This advisory does not address all potential violations or avenues of enforcement for the identified laws, nor does it identify all laws that may apply to AI.

and bias, and abuse of their data. Businesses must understand how the AI systems they utilize are trained, what information the systems consider, and how the systems generate output. They must also understand that they can be held accountable under tort, contract, or other laws if the employment of AI results in harm, particularly when AI systems are employed negligently or in use cases that could entail a level of risk. Developers and users of AI must also be transparent with consumers about whether consumer information is being used to train AI and how they are using AI to make decisions affecting consumers.

California's Consumer Protection, Civil Rights, and Competition Laws Provide Broad Protections

A. California's Unfair Competition Law

California's Unfair Competition Law protects the state's residents against unlawful, unfair, or fraudulent business acts or practices. (Bus. & Prof. Code, § 17200 et seq.) The law was intentionally written with broad, sweeping language to protect Californians from obvious and familiar forms of fraud and deception as well as new, creative, and cutting-edge forms of unlawful, unfair, and misleading behavior. (*People ex rel. Mosk v. Nat'l Research Co.* (1962) 201 Cal. App.2d 765, 772.) AI provides new tools for businesses and consumers alike, and also creates new opportunity to deceive Californians. Practices that deceive or harm consumers fall squarely within the purview of the Unfair Competition Law, and developers, entities that use AI, and end-users of AI systems should be aware that traditional consumer legal protections apply equally in the AI context.

In addition to prohibiting consumer deception, the Unfair Competition Law makes a violation of any other state, federal, or local law "independently actionable" under the Unfair Competition Law. (*Farmers Ins. Exchange v. Superior Court* (1994) 2 Cal.4th 377, 383.) Thus, the scope of the Unfair Competition Law is broad and incorporates numerous laws that may apply to AI in a variety of contexts.

For example, it may be unlawful under California's Unfair Competition Law to:[3]

- Falsely advertise the accuracy, quality, or utility of AI systems. This includes claiming that an AI system has a capability that it does not; representing that a system is completely powered by AI when humans are responsible for performing some of its functions; representing that humans are responsible for performing some of a system's functions when AI is responsible instead; or claiming without basis that a system is accurate, performs tasks better than a human would, has specified characteristics, meets industry or other standards, or is free from bias. (See, e.g., Bus. & Prof. Code, § 17500 et seq.; Civ. Code, § 1770 [The Consumer Legal Remedies Act].)

- Use AI to foster or advance deception. For example, the creation of deepfakes, chatbots, and voice clones that appear to represent people, events, and utterances that never existed or occurred would likely be deceptive.[4] Likewise, in many contexts it would likely be deceptive to fail to disclose that AI has been used to create a piece of media.

- Use AI to create and knowingly use another person's name, voice, signature, photograph, or likeness without that person's prior consent. (Civ. Code, §§ 3344, 3344.1; see also Civ. Code, § 1708.86 [prohibiting the creation and disclosure of sexually explicit material without the depicted person's consent]).[5]

- Use AI to impersonate a real person for purposes of harming, intimidating, threatening, or defrauding another person. (Pen. Code, § 528.5.)

- Use AI to impersonate a real person for purposes of receiving money or property. (Pen. Code, § 530; see also Pen. Code, § 529 [false personation of another in private or official capacity while doing specified acts].)

3 Many of the specific statutes listed in this advisory also provide for a private right of action.

4 See Michael Atleson, *Chatbots, deepfakes, and voice clones: AI deception for sale*, Federal Trade Commission Business Blog (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale.

5 Additional requirements for the use of AI in this context will go into effect on January 1, 2025—AB 2602 (Kalra) and AB 1836 (Bauer-Kahan)—and are described at page 8 below.

- Use AI to impersonate a real person for any unlawful purpose. (Pen. Code, § 530.5 [identity theft]; Pen. Code, § 530.55 [personal identifying information includes unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation]; see also *People v. Bollaert* (2016) 248 Cal.App.4th 699, 711-12 [unlawful purpose for identity theft includes intentional civil torts including invasion of privacy].)

- Use AI to impersonate a government official in the execution of official duties. (See Pen. Code, § 538d [impersonating a peace officer]; Pen. Code, § 146a [impersonating a state officer while committing specified acts]; Pen. Code, § 538f [impersonating a public utility officer]; Pen. Code, § 538g [impersonating a state/county/city/special district/city or county officer or employee].)

- Use AI in a manner that is unfair, including using AI in a manner that results in negative impacts that outweigh its utility, or in a manner that offends public policy, is immoral, unethical, oppressive, or unscrupulous, or causes substantial injury.

- Create, market, or disseminate an AI system that does not comply with federal or state laws, including the false advertising, civil rights, and privacy laws described below, as well as laws governing specific industries and activities.

Businesses may also be liable for supplying AI products when they know, or should have known, that AI will be used to violate the law. (See, e.g., *People v. Toomey* (1984) 157 Cal.App.3d 1, 15 [liability under section 17200 can be imposed for aiding and abetting].)

B. California's False Advertising Law

California's False Advertising Law provides another layer of protection for California's citizens against deceptive advertising. (Bus. & Prof. Code, § 17500 et seq.) The False Advertising Law "broadly prohibit[s] false or misleading advertising, declaring that it is unlawful for any person or business to make or distribute any statement to induce the public to enter into a transaction 'which is untrue or misleading, and which is known, or which by exercise of reasonable care should be known, to be untrue or misleading.'" (*Nationwide Biweekly Administration, Inc. v. Superior Court* (2020) 9 Cal.5th 279, 306 [quoting Bus. & Prof. Code, § 17500].) The law would prohibit false advertising regarding the capabilities, availability, and utility of AI products, the use of AI in connection with a good or service, as well as false advertising regarding any topic, whether or not it is generated by AI.

C. California's Competition Laws

California's competition laws, including the Cartwright Act, which prohibits anticompetitive trusts (Bus. & Prof. Code, § 16720), and the Unfair Practices Act, which regulates practices such as below-cost sales and loss leaders, protect California's economy. (Bus. & Prof. Code, § 17000 et seq.) The Unfair Competition Law, discussed above, also prohibits acts and practices that violate antitrust laws, among other practices. This includes, but is not limited to, conduct that threatens an incipient violation of an antitrust law, that violates the policy or spirit of one of those laws because its effects are comparable to a violation of the law, or that otherwise significantly threatens or harms competition.

AI developers and users should be aware of any risks to fair competition created by AI systems, such as those that set pricing. Even inadvertent harm to competition resulting from AI systems may violate one or more of California's competition laws. Anticompetitive actions by dominant AI companies may also harm competition in AI markets and violate both state and federal competition laws.

D. California's Civil Rights Laws

California's Unruh Civil Rights Act protects the freedom and equality of all people within the state, "no matter what their sex, race, color, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, sexual orientation, citizenship, primary language, or immigration status." (Civ. Code, § 51.) The California Fair Employment and Housing Act (FEHA) also protects Californians from harassment or discrimination in employment or housing based on a number of protected characteristics, including sex, race, disability, age, criminal history, and veteran or military status. (Gov. Code, § 12900 et seq.) Businesses may be liable for FEHA-prohibited discriminatory screening carried out by an agent, and further, the agents themselves may be directly liable to the individuals who

were discriminated against. (See *Raines v. U.S. Healthworks Medical Grp.* (2023) 15 Cal.5th 268, 291.) And Section 11135 prohibits denial of full and equal access to the benefits of, or discrimination under, any program or activity receiving state funds. (Gov. Code, § 11135.) This includes practices that, regardless of intent, have an adverse or disproportionate impact on members of a protected class, or create, reinforce, or perpetuate discrimination or segregation of members of a protected class. (Cal. Code of Regs., tit. 2, § 14027.)

We have seen AI systems incorporate societal and other biases into their decision-making.[6] Developers and users of AI should be wary of these potential biases that may be unlawfully impacting Californians.[7] Other laws also require that entities that take adverse action against citizens provide specific reasons for those adverse actions, including when AI was used to make the determination. As one example, the federal Fair Credit Reporting Act and Equal Credit Opportunity Act, as well as the California Consumer Credit Reporting Agencies Act, require such specific reasons be provided to Californians who receive adverse actions based on their credit scores. (See 15 U.S.C. § 1681 et seq.; 15 U.S.C. § 1691 et seq.; Civ. Code, § 1785.1 et seq.) The Consumer Financial Protection Bureau recently clarified that creditors who use AI or complex credit models must still provide individuals with specific reasons when they deny or take another adverse action against an individual.[8]

E. California's Election Misinformation Prevention Laws[9]

California law also provides guidance on a number of scenarios in which the use of AI may be illegal in the context of elections.[10] California law prohibits the use of undeclared chatbots with the intent to mislead a person about its artificial identity in order to incentivize a purchase or influence a vote in an election. (Bus. & Prof. Code, § 17941.) It is also impermissible to use AI to impersonate a candidate for elected office, or a candidate or initiative's website (Elec. Code, § 18320),[11] and to use AI to distribute, with actual malice, materially deceptive audio or visual media of a candidate for elective office within 60 days of that candidate's election with the intent to injure the candidate's reputation or deceive a voter into voting for or against the candidate. (Elec. Code, § 20010.)

6 See, e.g., Press Release, California Office of the Attorney General, Attorney General Bonta Launches Inquiry into Racial and Ethnic Bias in Healthcare Algorithms (Aug. 31, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare; Press Release, California Office of the Attorney General, Attorney General Bonta Welcomes Biden Administration's Effort to Increase Transparency, Combat Bias in Healthcare Algorithms (June 20, 2023), https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare.

7 See, e.g., National Institute of Science and Technology, *There's More to AI Bias Than Biased Data, NIST Report Highlights* (Mar. 16, 2022), https://www.nist.gov/news-events/news/2022/03/theres-more-ai-bias-biased-data-nist-report-highlights.

8 Consumer Financial Protection Circular 2023-03 (Sept. 19, 2023), https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/.

9 For more on Californians' voting rights, see Press Release, Ahead of General Election, Attorney General Bonta and Secretary of State Weber Remind Californians of Voting Rights and Advise Law Enforcement of Laws to Protect Voters (Oct. 3, 2024), https://oag.ca.gov/news/press-releases/ahead-general-election-attorney-general-bonta-and-secretary-state-weber-remind; see also California Department of Justice Law Enforcement Bulletin, Protecting California Voters from Election Interference and Voter Intimidation and Deception (Oct. 4, 2024), https://oag.ca.gov/system/files/attachments/press-docs/2024-dle-11.pdf.

10 For a description of new AI-related election laws see the discussion of AB 2355 (Carrillo) and AB 2655 (Berman) at page 8.

11 See Press Release, California Office of the Attorney General, Attorney General Bonta: Using Robocalls to Spread Disinformation is Unacceptable (Feb. 5, 2024), https://oag.ca.gov/news/press-releases/attorney-general-bonta-using-robocalls-spread-disinformation-unacceptable.

Data Protection Laws Provide Additional Broad Protections for Californians

Data is the bedrock underlying the massive growth in AI, and Californians' broad privacy and data rights directly impact AI systems, whether through the data used to build and train AI, or through the information that may be exposed by AI outputs.

Californians possess a constitutional right to privacy that applies to both government and private entities. (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 20.) Informational privacy, i.e., the "interest in precluding the dissemination or misuse of sensitive and confidential information" is a core privacy interest protected by the California Constitution. (*Id.* at 35.) Developers and entities that use AI must carefully monitor AI systems' training data, inputs, and outputs to ensure that Californians' constitutional right to privacy is respected.

The California Consumer Privacy Act (CCPA) broadly regulates the collection, use, sale, and sharing of consumers' personal information, including heightened protections for sensitive personal information. Personal information may also include inferences about consumers made by AI systems. (See Civ. Code, § 1798.140(v).) CCPA grants consumers important rights:

- The right to know about the personal information a business collects about them, and how it is used and shared;
- The right to correct inaccurate personal information that a business has about them;
- The right to delete personal information collected about them (with some exceptions);
- The right to opt out of the sale or sharing of their personal information; and
- The right to limit the use and disclosure of their sensitive personal information. (*Id.* § 1798.100 et seq.)

AI developers and users that collect and use Californians' personal information must comply with CCPA's protections for consumers, including by ensuring that their collection, use, retention, and sharing of consumer personal information is reasonably necessary and proportionate to achieve the purposes for which the personal information was collected and processed. (*Id.* § 1798.100.) Businesses are prohibited from processing personal information for non-disclosed purposes, and even the collection, use, retention, and sharing of personal information for disclosed purposes must be compatible with the context in which the personal information was collected. (*Ibid.*) AI developers and users should also be aware that using personal information for research is also subject to several requirements and limitations. (*Id.* § 1798.140(ab).) A new bill signed into law in September 2024 confirms that the protections for personal information in the CCPA apply to personal information in AI systems that are capable of outputting personal information. (Civ. Code, § 1798.140, added by AB 1008, Stats. 2024, ch. 804.) A second bill expands the definition of sensitive personal information to include "neural data." (Civ. Code, § 1798.140, added by SB 1223, Stats. 2024, ch. 887.)

The California Invasion of Privacy Act (CIPA) may also impact AI training data, inputs, or outputs. CIPA restricts recording or listening to private electronic communication, including wiretapping, eavesdropping on or recording communications without the consent of all parties, and recording or intercepting cellular communications without the consent of all parties. (Pen. Code, § 630 et seq.) CIPA also prohibits use of systems that examine or record voice prints to determine the truth or falsity of statements without consent. (*Id.* § 637.3.) Developers and users should ensure that their AI systems, or any data used by the system, do not violate CIPA.

California law contains heightened protection for particular types of consumer data, including education and healthcare data that may be processed or used by AI systems. The Student Online Personal Information Protection Act (SOPIPA) broadly prohibits education technology service providers from selling student data, engaging in targeted advertising using student data, and amassing profiles about students, except for specified school purposes. (Bus. & Prof. Code, § 22584 et seq.) SOPIPA applies to services and apps used primarily for "K-12 school purposes." This includes services and apps for home or remote instruction, as well as those intended for use at a public or private school. Developers and users should ensure any educational AI systems comply with SOPIPA, even if they are marketed directly to consumers.

Finally, the Confidentiality of Medical Information Act (CMIA) governs the use and disclosure of Californians' medical information and applies to businesses that offer software or hardware to consumers for the purposes of managing

medical information, or for diagnosis treatment, or management of medical conditions, including mobile applications or other related devices. (Civ. Code, § 56 et seq.) The rise of mental health and reproductive apps led to recent amendments to clarify that mental health and reproductive or sexual health digital services, such as apps and websites, are subject to the requirements of CMIA. Developers and users should ensure that any AI systems used for healthcare, including direct-to-consumer services, comply with the CMIA.

New California AI Laws

California has recently enacted the following legislation, effective January 1, 2025,[12] which addresses the use of AI and has broad impact for businesses and individuals:

Disclosure Requirements for Businesses

- **AB 2013 (Irwin**) requires AI developers to disclose information on their websites about their training data on or before January 1, 2026, including a high-level summary of the datasets used in the development of the AI system or service. (Civ. Code, § 3110 et seq.)
- **AB 2905 (Low)** requires telemarketing calls that use AI-generated or significantly modified synthetic marketing to disclose that use. (Pub. Util. Code, § 2874.)
- **SB 942 (Becker)** places obligations on AI developers, starting January 1, 2026, to make free and accessible tools to detect whether specified content was generated by generative AI systems. These developers are required to offer visible markings on AI-generated content to identify it as such and other detection features. (Bus. & Prof. Code, § 22757 et seq.)

Unauthorized Use of Likeness in the Entertainment Industry and Other Contexts

- **AB 2602 (Kalra)** requires that contracts authorizing the use of an individual's voice and likeness in a digital replica created through AI technology include a "reasonably specific description" of the proposed use and that the individual be represented by legal counsel or by a labor union. Absent these requirements, the contract is unenforceable, unless the uses are otherwise consistent with the terms of the contract and the underlying work. (Lab. Code, § 927.)
- **AB 1836 (Bauer-Kahan)** prohibits the use of a deceased personality's digital replica without prior consent within 70 years of the personality's death, imposing a minimum $10,000 fine for the violation. A deceased personality is any natural person whose name, voice, signature, photograph, or likeness has commercial value at the time of that person's death, or because of that person's death. (Civ. Code, § 3344.1.)

Use of AI in Election and Campaign Materials

- **AB 2355 (Carrillo)** requires any campaign advertisements generated or substantially altered using AI to include the following disclosure: "Ad generated or substantially altered using artificial intelligence." (Gov. Code, § 84504 et seq.)
- **AB 2655 (Berman)** requires that large online platforms (with at least one million California users) develop and implement procedures using state-of-the-art techniques to identify and remove certain materially deceptive election-related content—deepfakes—during specified periods before and after elections in California. It also requires certain additional content be labeled as manipulated, inauthentic, fake, or false during a longer period of time around elections in California. Platforms must provide an easy mechanism for California users to report the prohibited materials. (Code. Civ. Proc., § 35; Elec. Code, § 20510.)[13]

12 All bills discussed below become effective January 1, 2025. AB 2013 and SB 942 have additional operative dates, as specified, which determine when the laws impact covered entities and when violations of the provisions of the laws may be enforced.

13 A federal court has stayed enforcement of AB 2655 through June 28, 2025. (*Kohls v. Bonta* (E.D. Cal. Nov. 15, 2024, No. 2:24-cv-02527 JAM-CKD).) See also AB 2839 (Pellerin) prohibiting distribution of campaign or election-related materials that contain materially deceptive digital or audio media, including deepfake depictions of candidates, which was preliminarily enjoined by the same federal court on October 2, 2024. (*Ibid.* (Oct. 2, 2024).)

Expanded Prohibitions and Reporting of Exploitative Uses of AI

- **AB 1831 (Berman)** and **SB 1381 (Wahab)** expands existing criminal prohibitions on child pornography to include the use of AI in the creation of visual depictions of the sexual abuse and exploitation of children. (Pen. Code, §§ 311, 311.2, 311.3, 311.4, 311.11, 311.12, 312.3.)
- **SB 926 (Wahab)** extends criminal penalties to the creation of nonconsensual pornography using deepfake technology. (Pen. Code, § 647.)
- **SB 981 (Wahab)** requires social media platforms to provide a mechanism for California users to report sexually explicit digital identity theft or deepfake pornography. (Bus. & Prof. Code, § 22670 et seq.)

Supervision of AI Tools in Healthcare Settings

- **SB 1120 (Becker)** requires health insurers to ensure that licensed physicians supervise the use of AI tools that make decisions about healthcare services and insurance claims. (Health & Saf. Code, § 1367.01; Ins. Code, § 10123.135.)

Entities Should Remain Vigilant About Other Laws and Regulations Which May Be Applicable to AI Technologies

Beyond the laws and regulations discussed in this advisory, other California laws—including tort, public nuisance, environmental and business regulation, and criminal law—apply equally to AI systems and to conduct and business activities that involve the use of AI. Conduct that is illegal if engaged in without the involvement of AI is equally unlawful if AI is involved, and the fact that AI is involved is not a defense to liability under any law.

This overview is not intended to be exhaustive. Entities that develop or use AI have a duty to ensure that they understand and are in compliance with all state, federal, and local laws that may apply to them or their activities. That is particularly so when AI is used or developed for applications that could carry a potential risk of harm to people, organizations, physical or virtual infrastructure, or the environment.